Identity-Based Non-Interactive Key Sharing Equivalent to RSA Public-Key Cryptosystem

Hatsukazu TANAKA
Department of Electrical & Electronics Engineering
Faculty of Engineering, Kobe University
Rokko, Nada, Kobe, Japan 657
E-mail : tanaka@eedept.kobe-u.ac.jp

Abstract — **A new simply implemented identity-based non-interactive key sharing scheme (ID-NIKS) has been proposed. The security depends on the difficulty of factoring and is equivalent to RSA public-key cryptosystem even when the collusion among users is performed. The center algorithm is very simple and easily implemented. The extension to a common-key sharing scheme among multi-users is also possible.**

I. Introduction

In this paper a new identity-based non-interactive key sharing scheme (ID-NIKS) has been proposed in order to realize the original elegant concept of identity-based cryptosystem[1]. The security of our proposed ID-NIKS depends on the difficulty of factoring and is equivalent to RSA public-key cryptosystem[2] even when the collusion among users is performed. The center algorithm is very simple and easily implemented.

II. Basic Center Algorithm

Let $P = 2p + 1$ and $Q = 2q + 1$ (p, q:primes) be two large Sophie Germain's (S.G.) primes and their product be $N = PQ$. The Carmichael function of N is given by L=lcm $\{P-1, Q-1\} = 2pq$. Let ID_l be a user l's (l=A,B,C,....) identity information. Let f and h be two one-way hash functions which produce from ID_l the following $r(\geq 2)$-ary m-dimensional non-zero vector $\mathbf{v}_l^{(f)}$, of which weight sum is $w_l(>0)$, and $r(\geq 2)$-ary n-dimensional non-zero vector $\mathbf{v}_l^{(h)}$, of which weight sum is an odd number e_l much less than $\min\{p, q\}$, respectively, i.e. $f(ID_l) = \mathbf{v}_l^{(f)} = (l_0^{(f)}, l_1^{(f)}, l_2^{(f)}, ..., l_{m-1}^{(f)})$, $l_k^{(f)} \in Z_r (r \geq 2)$, $\sum_{k=0}^{m-1} l_k^{(f)} = w_l$ and $h(ID_l) = \mathbf{v}_l^{(h)} = (l_0^{(h)}, l_1^{(h)}, l_2^{(h)}, ..., l_{n-1}^{(h)})$, $l_j^{(h)} \in Z_r (r \geq 2)$, $\sum_{j=0}^{n-1} l_j^{(h)} = e_l$, if e_l=even number, then $l_{n-1}^{(h)} \rightarrow l_{n-1}^{(h)} + 1$. Then we can calculate the inverse element d_l of e_l such that $e_l d_l = 1 \pmod{L}$ because $\gcd\{e_l, L\} = 1$.

Here we introduce two sets of n-random numbers $X = \{x_0, x_1, ..., x_{n-1}\}$ and $Y = \{y_0, y_1, ..., y_{n-1}\}$, and a set of m-random numbers $Z = \{z_0, z_1, ..., z_{m-1}\}$. Then calculate the following equations: $X_l = \sum_{j=0}^{n-1} l_j^{(h)} x_j \pmod{L}$, $Y_l = \prod_{j=0}^{n-1} y_j^{l_j^{(h)}} \pmod{N}$, $Z_l = \sum_{k=0}^{m-1} l_k^{(f)} z_k \pmod{N}$ and

$$g_l(j,k) = \left(Y_l^{x_j} y_j^{X_l}\right)^{d_l} \left(w_l z_k + Z_l\right) \pmod{N} \quad (1)$$

to obtain an $n \times m$ matrix $G_l = [g_l(j,k);\ 0 \leq j \leq n-1,\ 0 \leq k \leq m-1,\ l$ = A,B,C,.....].

Finally the trusted center publishes $\{N, f, h, ID_l$ (l =A,B,C,.....)$\}$ and delivers G_l to each user l through a secure channel or by an IC card.

III. Non-Interactive Key Sharing

We assume here that two users A and B want to share a common-key K_{AB} between them non-interactively. First A calculates $f(ID_B) = \mathbf{v}_B^{(f)}$ and $h(ID_B) = \mathbf{v}_B^{(h)}$ from ID_B using two one-way hash functions f and h. Then A executes the following simple calculation mod N to share a common-key K_{AB} with B.

$$K_{AB}^{(A)} = \left[\prod_{j=0}^{n-1}\left\{\sum_{k=0}^{m-1} b_k^{(f)} g_A(j,k)\right\}^{b_j^{(h)}}\right]^{e_A}$$
$$= \left\{\left(Y_A^{X_B} Y_B^{X_A}\right)^{d_A d_B} \left(w_A Z_B + w_B Z_A\right)\right\}^{e_A e_B} \quad (2)$$

Similarly B calculates $f(ID_A) = \mathbf{v}_A^{(f)}$ and $h(ID_A) = \mathbf{v}_A^{(h)}$ from ID_A using two one-way hash functions f and h. Then B executes the following simple calculation mod N to share a common-key K_{AB} with A.

$$K_{AB}^{(B)} = \left[\prod_{j=0}^{n-1}\left\{\sum_{k=0}^{m-1} a_k^{(f)} g_B(j,k)\right\}^{a_j^{(h)}}\right]^{e_B}$$
$$= \left\{\left(Y_B^{X_A} Y_A^{X_B}\right)^{d_B d_A} \left(w_B Z_A + w_A Z_B\right)\right\}^{e_B e_A} \quad (3)$$

Hence their shared common-key is given by

$$K_{AB} = M_{AB}^{e_A e_B} \pmod{N} \quad (4)$$

where $M_{AB} = \left(Y_A^{X_B} Y_B^{X_A}\right)^{d_A d_B} \left(w_A Z_B + w_B Z_A\right) \pmod{N}$.

IV. Considerations on the Security

One strategy to forge a common-key between any pair of third parties is to solve the equation (1) gathered by the user's collusion in $y_j^{x_i}$ and z_k, and then forge a common-key $K_{\alpha\beta}$ between α and β. The other strategy to forge a common-key between any pair of third parties is to solve directly the key generation equations

$$K_{l\alpha} = K_{\alpha l} = \left[\prod_{j=0}^{n-1}\left\{\sum_{k=0}^{m-1} l_k^{(f)} g_\alpha(j,k)\right\}^{l_j^{(h)}}\right]^{e_\alpha} \pmod{N} \quad (5)$$

in $g_\alpha(j,k)$, gathered by user's collusion among l = A,B,C, .., and then to forge a common-key $K_{\alpha\beta}$ between α and β.

However, both strategies are impossible to execute because of the assumption that it is extremely difficult to break the RSA public-key cryptosystem.

References

[1] A.Shamir, "Identity-based cryptosystems and signature schemes," *Advances of Cryptology - Crypto'84*, LNCS vol.196, pp.47-53, 1985.

[2] R.L.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public-key cryptosystem," *Communications of ACM*, vol.21, pp.120-126, 1978.

0-7803-5000-6/98/$10.00 © 1998 IEEE.